This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A[[n]] ~~authentication~~ system for authenticating a user's signature, the system comprising:

[[a]] first extraction means for extracting first angle data and first distance data relating to different parts of the user's signature to obtain a signature trace;

normalization means for generating a normalized signature trace by determining a plurality of temporally equidistant points on the signature trace ~~by normalizing the signature trace~~ such that ~~to~~ an arc length of the signature trace is a unit measurement of length ~~of 1~~ and a total time to produce the signature is a unit measurement of time ~~to 1~~;

[[a]] second extraction means for extracting second angle data and second distance data relating to different parts of the normalized signature trace, wherein the second angle data and second distance data are selected such that variance between signatures from the user is minimized and variance between signatures from other users is maximized;

registration means for ~~setting up~~ storing a reference data file comprising reference angle data and reference distance data extracted from a plurality of samples of the user's signature;

comparison means for comparing the data extracted by the second extraction means during an authentication phase to the reference angle data and the reference distance data ~~held~~ stored in the reference data file, according to predefined verification criteria; and

verification means for ~~providing~~ generating an output indicative of a[[n]] ~~appropriate~~ match between the user's signature and the reference angle data and reference distance data in dependence on ~~the result of the comparison~~ said comparing.

2. (Currently Amended) [[A]] The system according to claim 1, wherein the second extraction means is adapted to extract data relating to a plurality of different points of the user's signature including data relating some of said points to other points in the user's signature ~~as inputted into the system by the manual input device~~.

3. (Currently Amended) [[A]] The system according to claim 2, wherein the second extraction means is adapted to extract data relating to a plurality of different points of the user's signature including data relating each of a number of said points to an immediately preceding point in the user's signature ~~as inputted into the system by the manual input device~~.

4. (Currently Amended) [[A]] The system according to claim 2 ~~or 3~~, wherein the second extraction means is adapted to extract data relating to a plurality of different points of the user's signature including data relating a last point to a first point in the user's signature ~~as inputted into the system by the manual input device~~.

5. (Currently Amended) [[A]] The system according to claim 1, wherein the second extraction means includes angle extraction means for extracting angle data concerning the relative angular positions of a plurality of points of the user's signature.

6. (Currently Amended) [[A]] The system according to claim 1, wherein the second extraction means includes distance extraction means for extracting distance data concerning the relative distances apart of a plurality of points of the user's signature.

7. (Currently Amended) [[A]] The system according to claim 1, wherein the second extraction means includes timing extraction means for extracting timing data indicative of the relative times between execution of different parts of the user's signature, and the comparison means is adapted to compare the extracted timing data with reference timing data in the reference data file.

8. (Currently Amended) [[A]] The system according to claim 1, ~~wherein~~ further comprising password verification means ~~is provided~~ for verifying ~~input of a required~~ a user password~~, as determined by reference password means, by the user using a keyboard input device~~.

9. (Currently Amended) [[A]] The system according to claim 8, ~~wherein~~ further comprising timing verification means ~~is provided~~ for verifying ~~input of~~ that the password is input in accordance with a predetermined ~~by the user with the required~~ timing~~, as determined by reference timing means, using the keyboard input device~~.

10. (Currently Amended) [[A]] The system according to claim 9, wherein the timing verification means includes means for verifying a plurality of hold times for which the relevant keys of the keyboard input device are depressed during input of the password, and means for verifying a plurality of latency times between a release of one key and a depression of a following key during use of the keyboard input device to enter the password.

11. (Currently Amended) [[A]] The system according to claim 1, ~~wherein~~ further comprising user name input means ~~is provided~~ for receiving a user name ~~inputted into the system to identify the identity of the user for the purposes of selection of the required reference data file for that user~~.

12. (Currently Amended) [[A]] The system according to claim 1, wherein the comparison means incorporates at least one neural network for determining the predefined verification criteria ~~by which a match is to be judged by providing a comparison output to the verification means~~.

13. (Currently Amended) [[A]] The system according to claim 1, wherein the second extraction means is adapted to extract data relating to different features of the user's signature selected according to ~~the~~ a fitness of such features to discriminate the user's signature for the purposes of verification and determined by a fitness function relating ~~the~~ a relative fitness of the features to their form and number.

14. (Currently Amended) [[A]] The system according to claim 13, wherein the fitness function is optimized by an optimization algorithm~~, such as a genetic algorithm~~.

15. (Currently Amended) [[A]] The system according to claim 1, further comprising [[a]] training means for training the system to refine the predefined verification criteria ~~by which a match is to be judged on the basis of~~ using angle and distance data relating to a plurality of samples of the user's signature inputted into the system by the user during the registration phase and generated false samples.

16. (Currently Amended) [[A]] The system according to claim 1, wherein the verification means is adapted to provide an ~~reject~~ output indicative of a non-match~~ing of one or more verification criteria only after completion of all the verification procedures~~.

17. (Currently Amended) A method for authenticating a user's signature, comprising:

extracting first angle data and first distance data relating to different parts of the user's signature inputted into the system by a manual input device to obtain a signature trace;

normalizing the signature trace to generate a plurality of temporally equidistant points on the signature trace ~~by normalizing the signature trace~~ such that ~~to~~ an arc length of the signature trace is a unit measurement of length ~~of 1~~ and a total time to produce the signature is a unit measurement of time ~~to 1~~;

using a computing device, extracting second angle data and second distance data relating to different parts of the normalized signature trace, wherein the second angle data and second distance data are selected such that variance between signatures from the user is minimized and variance between signatures from other users is maximized;

creating a reference data file comprising reference angle data and reference distance data extracted from a plurality of samples of the user's signature ~~inputted into the system by the user using a manual input device during a registration phase~~;

comparing the data relating to different parts of the normalized signature trace during an authentication phase to the reference angle and the reference distance data ~~held~~ stored in the reference data file, according to predefined verification criteria; and

~~providing~~ generating an output indicative of a[[n]] ~~appropriate~~ match between the user's signature and the reference angle data and reference distance data in dependence on ~~the result of the comparison~~ said comparing.

18. (Currently Amended) The method of claim 17, wherein said extracting said first angle data and first distance data comprises extracting data relating to a plurality of different points of the user's signature including data relating some of said points to other points in the user's signature ~~as inputted into the system by the manual input device~~.

19. (Currently Amended) The method of claim 18, wherein said extracting said first angle data and first distance data comprises extracting data relating to a plurality of different points of the user's signature including data relating each of a number of said points to an immediately preceding point in the user's signature ~~as inputted into the system by the manual input device~~.

20. (Currently Amended) The method according to claim 18 ~~or 19~~, wherein extracting said first angle data and first distance data comprises extracting data relating to a plurality of different points of the user's signature including data relating a last point to a first point in the user's signature ~~as inputted into the system by the manual input device~~.

21. (Currently Amended) The method of claim 17, wherein extracting said first angle data and first distance data includes extracting angle data concerning the relative angular positions of a plurality of points of the user's signature.

22. (Currently Amended) The method of claim 17, wherein extracting said first angle data and first distance data includes extracting distance data concerning the relative distances apart of a plurality of points of the user's signature.

23. (Currently Amended) The method of claim 17, wherein extracting said first angle data and first distance data includes extracting timing data indicative of the relative times between

execution of different parts of the user's signature, and ~~the comparison means is adapted to~~ said comparing further comprises comparing ~~compare~~ the extracted timing data with reference timing data in the reference data file.

24. (Currently Amended) The method of claim 17, further comprising verifying ~~an input of~~ a ~~required~~ password~~, as determined by reference password, by the user using a keyboard input device~~.

25. (Currently Amended) The method of claim 24, further comprising verifying the ~~input of the~~ password ~~by the user with a required~~ using a predefined timing~~, as determined by a reference timing, using the keyboard input device~~.

26. (Previously presented) The method of claim 25, wherein verifying the input further comprises:

verifying a plurality of hold times for which the relevant keys of the keyboard input device are depressed during input of the password; and

verifying a plurality of latency times between the release of one key and the depression of the following key during use of the keyboard input device to enter the password.

27. (Currently Amended) The method of claim 17, further comprising receiving a user name ~~inputted into the system to identify the identity of the user for the purposes of selection~~ and using the user name to identify a ~~of the required~~ reference data file ~~for that user~~.

28. (Currently Amended) The method of claim 17, wherein said comparing the angle and distance data incorporates at least one neural network for determining the predetermined verification criteria ~~by which a match is to be judged by providing a comparison output to the verification means~~.

29. (Currently Amended) The method of claim 17, wherein said extracting said first angle data and said first distance data ~~extracts~~ further comprises extracting data relating to different features of the user's signature selected according to the fitness of such features to discriminate the user's signature for the purposes of verification and determined by a fitness function relating the relative fitness of the features to their form and number.

30. (Currently Amended) The method of claim 29, wherein the fitness function is optimized by an optimization algorithm~~, such as a genetic algorithm~~.

31. (Currently Amended) The method of claim 17, further comprising training to refine the predefined verification criteria ~~by which a match is to be judged~~ on the basis of angle and distance data relating to a plurality of samples of the user's signature inputted by the user during the registration phase and generated false samples.

32. (Currently Amended) The method of claim 17, wherein said generating ~~providing verification of the user's signature provides a reject~~ further comprises generating an output indicative of a non-match~~ing of one or more verification criteria only after completion of all the verification procedures~~.

33. (Currently Amended) A method for authenticating a user's signature, comprising:

extracting first angle data and first distance data relating to different parts of a user's signature inputted using a manual input device to obtain a signature trace;

normalizing the signature trace to generate a plurality of temporally equidistant points on the signature trace ~~by normalizing the signature trace~~ such that ~~to~~ an arc length of the signature trace is a unit measurement of length ~~of 1~~ and a total time to produce the signature is a unit measurement of time ~~to 1~~; and

using a computing device, extracting second angle data and second distance data relating to different parts of the normalized signature trace, wherein the second angle data and second

distance data are selected such that variance between signatures from the user is minimized and variance between signatures from other users is maximized.

34. (Currently Amended) The method of claim 33, further comprising:

~~setting up~~ storing a reference data file comprising reference angle data and reference distance data relating to a plurality of samples of the user's signature inputted during a registration phase, wherein the plurality of samples of the user's signature are normalized based upon a time to obtain a plurality of normalized samples.

35. (Currently Amended) The method of claim 34, further comprising:

comparing the angle and distance data relating to different parts of the normalized signature trace during an authentication phase to the reference angle and the reference distance data held in the reference data file, according to predefined verification criteria.

36. (Currently Amended) The method of claim 35, further comprising:

~~providing~~ generating an output indicative of a[[n]] ~~appropriate~~ match between the user's signature and the reference angle data and reference distance data in dependence on the result of the comparison, thereby providing verification of the user's signature.

37. (Currently Amended) The method of claim 34, further comprising:

training to refine the predefined verification criteria by which a match is to be judged on the basis of angle and distance data relating to a plurality of samples of the user's signature during the registration phase and generated false samples.

38. (Currently Amended) A computer-readable storage medium having computer-readable instructions stored thereon for authenticating a user's signature, the computer-readable instructions comprising ~~instructions for~~:

instructions for extracting first angle data and first distance data relating to different parts of a user's signature ~~inputted~~ to obtain a signature trace;

instructions for normalizing the signature trace to generate a plurality of temporally equidistant points on the signature trace ~~by normalizing the signature trace~~ such that ~~to~~ an arc length of the signature trace is a unit measurement of length ~~of 1~~ and a total time to produce the signature is a unit measurement of time ~~to 1~~; and

instructions for extracting second angle data and second distance data relating to different parts of the normalized signature trace, wherein the second angle data and second distance data are selected such that variance between signatures from the user is minimized and variance between signatures from other users is maximized.

39. (Currently Amended) The computer-readable storage medium of claim 38, further comprising ~~instructions for~~:

~~setting up~~ instructions for storing a reference data file comprising reference angle data and reference distance data extracted from a plurality of samples of the user's signature inputted using a manual input device during a registration phase, wherein the plurality of samples of the user's signature are normalized based upon a time to obtain a plurality of normalized samples.

40. (Currently Amended) The computer-readable storage medium of claim 39, further comprising ~~instructions for~~:

instructions for comparing the data relating to different parts of the normalized signature trace during an authentication phase to the reference angle and the reference distance data held in the reference data file, according to predefined verification criteria.

41. (Currently Amended) The computer-readable storage medium of claim 40, further comprising ~~instructions for~~:

~~providing~~ instructions for generating an output indicative of a[[n]] ~~appropriate~~ match between the user's signature and the reference angle data and reference distance data in dependence on the result of the comparison, thereby providing verification of the user's signature.

42. (Currently Amended) The computer-readable storage medium of claim 39, further comprising ~~instructions for~~:

instructions for training to refine the predefined verification criteria by which a match is to be judged on the basis of angle and distance data relating to a plurality of samples of the user's signature during the registration phase and generated false samples.

43. (Currently Amended) A system for authenticating a user's signature, the system comprising:

an input apparatus, wherein the input apparatus is configured to provide an output indicative of the location of the input apparatus with respect to time when the input apparatus is manipulated;

a computing apparatus, wherein the computing apparatus is configured to:

extract first angle data and first distance data relating to different parts of a user's signature output~~ted~~ by the input apparatus to obtain a signature trace;

normalize the signature trace to generate a plurality of temporally equidistant points on the signature trace ~~by normalizing the signature trace~~ such that ~~to~~ an arc length of the signature trace is a unit measurement of length ~~of 1~~ and a total time to produce the signature is a unit measurement of time ~~to 1~~; and

extract second angle data and second distance data relating to different parts of the normalized signature trace, wherein the second angle data and second distance data are selected such that variance between signatures from the user is minimized and variance between signatures from other users is maximized.

44. (Previously presented) The system of claim 43, further comprising:

a reference data file comprising reference angle data and reference distance data relating to a plurality of samples of the user's signature inputted using a manual input device during a registration phase, wherein the plurality of samples of the user's signature are normalized based upon a time to obtain a plurality of normalized samples.

45. (Currently Amended) The system of claim 44, further comprising:

a comparator apparatus configured to compare the data relating to different parts of the normalized signature trace during an authentication phase the reference angle and the reference distance data held in the reference data file, according to predefined verification criteria.

46. (Currently Amended) The system of claim 45, further comprising:

an output apparatus configured to provide an output indicative of a[[n]] ~~appropriate~~ match between the user's signature and the reference angle data and reference distance data in dependence on the result of the comparison, thereby providing verification of the user's signature.

47. (Currently Amended) The system of claim 44, further comprising:

a trainer configured to refine the predefined verification criteria by which a match is to be judged on the basis of angle and distance data relating to a plurality of samples of the user's signature during the registration phase and generated false samples.

48. (Currently Amended) A method of verifying a user's signature, comprising:

using a computing device, comparing data derived from at least one vector from an input signature received from a manual input device during an authentication phase to reference angle data and reference distance data, according to predefined verification criteria, wherein the data derived from said at least one vector comprises data relating to different parts of a normalized signature trace, wherein an arc length and total time of the signature trace are normalized to [[1]] unit measurements to generate a plurality of temporally equidistant points on the signature trace, and wherein the reference angle data and reference distance data is obtained from a reference data file comprising data relating to a plurality of samples of the user's signature, wherein the plurality of samples of the user's signature are normalized based upon a time to obtain a plurality of normalized samples and selected such that variance between signatures from the user is minimized and variance between signatures from other users is maximized; and

providing an output indicative of a[[n]] ~~appropriate~~ match between the data derived from said at least one vector and the reference angle data and reference distance data ~~in dependence on the result of the comparison, thereby providing verification of the user's signature~~.

49. (Previously presented) The method of claim 48, wherein the data derived from said least one vector relates to different features of the user's signature selected according to the fitness of such features to discriminate the user's signature for the purposes of verification and determined by a fitness function relating the relative fitness of the features to their form and number.

50. (Currently Amended) The method of claim 49, wherein the fitness function is optimized by an optimization algorithm~~, such as a genetic algorithm~~.

51. (Currently Amended) The method of claim 48, further comprising:

training to refine ~~the~~ verification criteria by which [[a]] said match is to ~~be judged~~ determined ~~on the basis of data relating to a plurality of samples of the user's signature during the registration phase and generated false samples~~.

52. (Currently Amended) The method of claim 48, further comprising verifying an input of a required password, as determined by a reference password~~, by the user using a keyboard input device~~.

53. (Currently Amended) The method of claim 52, further comprising verifying the input of the password ~~by the user~~ with a required timing, as determined by a reference timing~~, using the keyboard input device~~.

54. (Previously presented) The method of claim 53, wherein verifying the input further comprises:

verifying a plurality of hold times for which relevant keys of ~~the keyboard~~ an input device are depressed during input of the password; and

verifying a plurality of latency times between the release of one key and the depression of the following key during use of the ~~keyboard~~ input device to enter the password.

55. (Currently Amended) A method of verifying a signature, comprising:

receiving, from a manual input device, the signature;

extracting first angle data and first distance data relating to different parts of the signature to obtain a signature trace;

normalizing the signature trace to generate a plurality of temporally equidistant points on the signature trace ~~by normalizing the signature trace~~ such that ~~to~~ an arc length of the signature trace is a unit measurement of length ~~of 1~~ and a total time to produce the signature is a unit measurement of time ~~to 1~~;

using a computing device, extracting second angle data and second distance data relating to different parts of the normalized signature trace, wherein the second angle data and second distance data are selected such that variance between signatures from the user is minimized and variance between signatures from different users is maximized;

~~setting up~~ storing a reference data file comprising reference angle data and reference distance data extracted from a plurality of samples of the user's signature input~~ted into the system by the user~~ during a registration phase;

comparing the data relating to different parts of the normalized signature trace during an authentication phase to the reference angle data and the reference distance data ~~held~~ stored in the reference data file, according to defined verification criteria; and

providing an output to the user indicative of a[[n]] ~~appropriate~~ match between user's signature and the reference angle data and reference distance data in dependence on the result of said comparing ~~the comparison~~.

56. (Previously presented) The method of claim 55, further comprising linearly time warping the signature trace so that the normalized signature trace contains a pre-determined number of temporally equidistant points.

57. (Previously presented) The system of claim 1, wherein the first extraction means extracts at least one vector to derive the angle data and distance data.

58. (New) The system according to claim 1, wherein the second extraction means is adapted to extract data according to a fitness determined by applying a genetic algorithm to pairs of said temporally equidistant points.